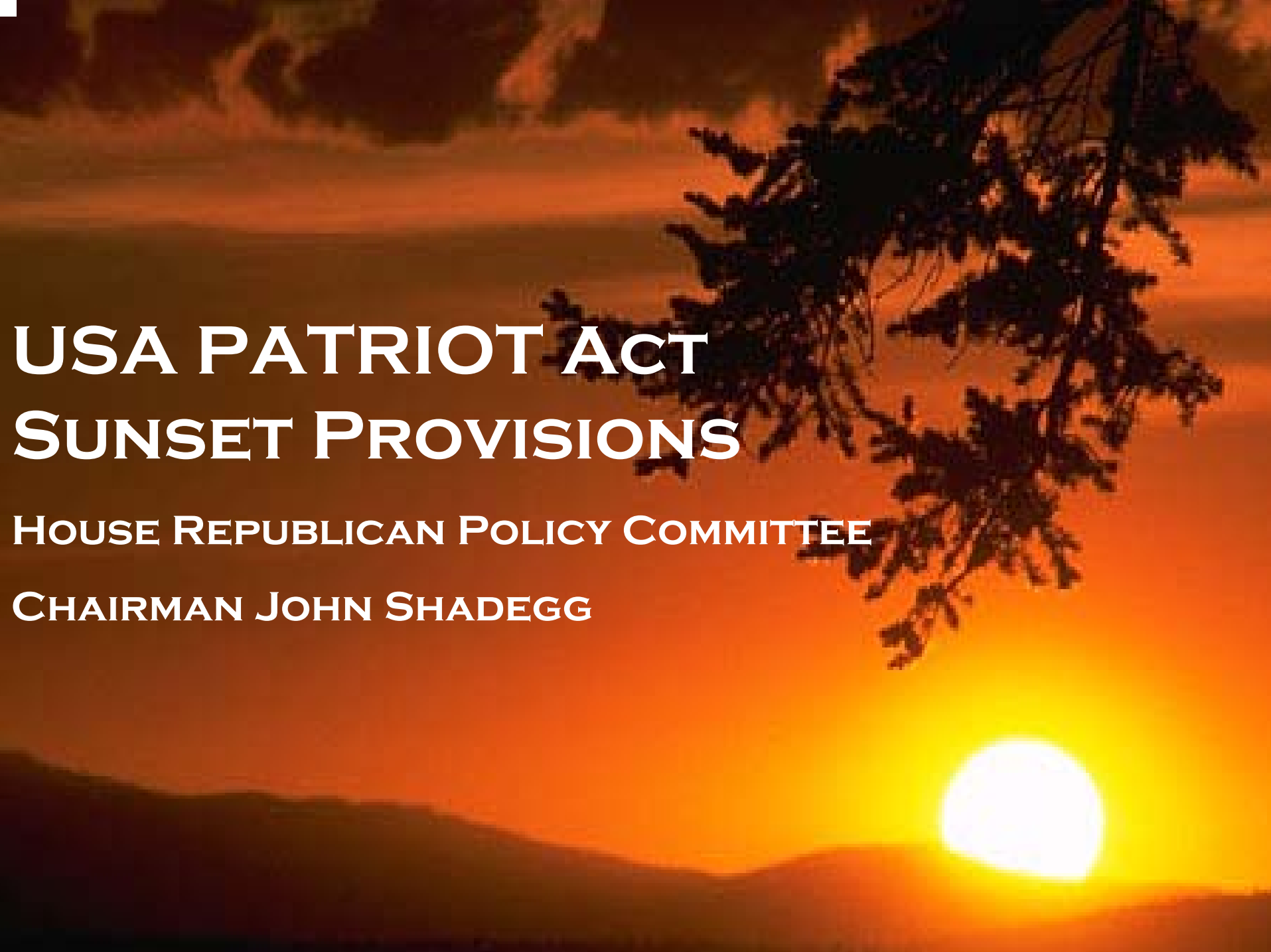

USA PATRIOT Act Sunset Provisions

House Republican Policy Committee

Chairman John Shadegg

USA PATRIOT Act Sunset Provisions

Sections 201 and 202: Authority to intercept wire, oral, and electronic communications relating to terrorism and computer fraud and abuse offenses, respectively.

Subsections 203(b) and (d): Authority to share electronic, wire, and oral interception information, and general foreign intelligence information, respectively.

Section 204: Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

Section 206: Roving surveillance authority under the Foreign Intelligence Surveillance Act (FISA) of 1978.

Section 207: Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

Section 209: Seizure of voice-mail messages pursuant to warrants.

Section 212: Emergency disclosure of electronic surveillance.

Section 214: Pen register and trap and trace authority under FISA.

Section 215: Access to records and other items under the Foreign Intelligence Surveillance Act.

Section 217: Interception of computer trespasser communications.

Section 220: Nationwide service of search warrants for electronic evidence.

Section 223: Civil liability for certain unauthorized disclosures.

Section 218: Foreign intelligence information ("the wall").

Section 225: Immunity for compliance with FISA wiretap.

Section 6001 of P.L. 108-458: Individual terrorists as agents of foreign powers.

House Republican Policy Committee
Chairman John Shadegg

Sunset Provisions

- Subsection 224(a) of Title II of the Act directs that various sections are to remain in effect until December 31, 2005.

- Subsection 224(b) creates two exceptions to this sunset provision with respect to:
  - Any particular foreign intelligence investigation that began before December 31, 2005.
  - Any particular offense or potential offense that began or occurred before December 31, 2005.

Section 201

- Section 201 adds the following crimes to the federal wiretap predicate offense list:
  - 18 U.S.C. 229 (chemical weapons)
  - 2332 (crimes of violence committed against Americans overseas)
  - 2332a (weapons of mass destruction)
  - 2332b (multinational terrorism)
  - 2332d (financial transactions with a country designated a sponsor of terrorism)
  - 2339A (providing material support to a terrorist)
  - 2339B (providing material support to a terrorist organization)

Section 202

- Section 202 adds the following crimes to the federal wiretap predicate offense list:
  - 18 U.S.C. 1030 (computer fraud and abuse).

Subsection 203(b)

- Subsection 203(b) amends federal wiretap law to permit law enforcement officials to disclose wiretap evidence to various federal officials including law enforcement, intelligence, protective, immigration, national defense, and national security officials when it involves foreign intelligence, counterintelligence, or foreign intelligence information.

- Subsection 203(b) provides the authority to share electronic, wire, and oral interception information.
  - Prior to the act, there was no explicit authorization for disclosure to intelligence officials.

Subsection 203(d)

- Subsection 203(d) provides the general authority to share foreign intelligence information.

- Subsection 203(d) authorizes law enforcement officers to share foreign intelligence, counterintelligence, and foreign intelligence information with federal officials notwithstanding any other legal restriction.

Section 204

- Section 204 clarifies intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

- Under the federal wiretap law, the general prohibitions against wiretapping, and against the acquisition of communications records and stored electronic communications, do not preclude foreign intelligence gathering activities in international or foreign communications systems.

- Section 204 clarifies that the general trap and trace device and pen register prohibitions do not preclude use of these devices to gather foreign intelligence information.

Section 209

- Prior to enactment of the Act, some federal courts required a wiretap order rather than a search warrant for authorities to seize unretrieved voice mail.

- Section 209 treats voice mail like e-mail, subject to seizure under a search warrant rather than a more demanding wiretap order.

Section 212

- Section 212 authorizes electronic communications service providers to disclose the communications (or records relating to such communications) of their customers or subscribers if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure.
  - The Homeland Security Act repealed the content provision of this section and enacted a separate content provision, 18 U.S.C. 2702(b)(7), but did not address customer records. Thus, the records provision will sunset on December 31, 2005 but the content provision will remain in effect.
- Prior law limited the circumstances under which service providers might disclose the particulars of a customer's transaction records or communications without a warrant, a court order, or the customer's consent.

Section 217

- Section 217 allows victims of computer attacks by cyber-terrorists and others to ask law enforcement officers to monitor trespassers in their systems.

- Federal wiretap law proscribes the interception of telephone, face to face, or computer conversations, subject to certain narrow exceptions such as the issuance of a wiretap order, the consent of one of the participants in the conversation, or a communications carrier's protection of its property.

Section 220

- Section 220 authorizes the court in the district where a crime occurred to issue search warrants or orders to be served anywhere in the country for access to electronic communications content and customer record information.

- Before the act, federal authorities could only gain access to a communications service provider's customer records and the content of their electronic communications through a search warrant or court order issued in the judicial district in which it was to be executed.

Section 223

- Section 223 confirms the authority of agency heads to discipline federal officers and employees for willful or intentional violations of federal wiretap or stored communications law.

- It also imposes civil liability for any willful use or disclosure of information beyond that which is authorized.
  - Unrelated to section 223, federal law imposes criminal penalties for illegal wiretapping, unlawful access to store communications (e.g., e-mail or voice mail), or illegally using a pen register or trap and trace device.

Section 206

- Prior to the Act, the government could seek information and assistance from common carriers, landlords, custodians, and other individuals specified in FISA surveillance orders.

- Section 206 amends FISA to permit a general command for assistance where the target of the surveillance has taken steps to thwart the identification of any specific person.
  - The law enforcement wiretap statute has a similar provision for law enforcement orders.

Section 207

Before the PATRIOT Act:

- Prior to the act, FISA wiretap orders with the agent of a foreign power as their target had a maximum duration of 90 days, and could be extended in 90 day increments.
- Also, before the act was passed, FISA physical search orders were good for no more than 45 days (but up to one year if a foreign power was the target).

After the PATRIOT Act:

- FISA wiretap orders relating to the agent of foreign power may remain in effect for up to 120 days and may be extended at one year intervals.
- FISA physical search orders and extensions may be authorized for 90 days (unless they target a foreign power), but orders with an agent of a foreign power as their target may be issued for up to 120 days with extensions for up to one year.

Section 214

Before the PATRIOT Act:

- FISA allows pen register or trap and trace device order for telephone communications in order to acquire information relevant to a foreign intelligence or international terrorism investigation.
- Upon the additional certification that the communications monitored would likely be either:
  - Those of an international terrorist or spy.
  - Those of a foreign power or its agent relating to the criminal activities of an international terrorist or spy.

After the PATRIOT Act:

- Section 214 expands the FISA pen register/ trap and trace device procedure to both wire and electronic communications (i.e. telephone, e-mail, Internet communications).
- It drops the requirement that the communications be those of international terrorists or spies or be related to criminal activities.

Section 215

- Prior to the Act, authorities could obtain a FISA court order for access to the business records of hotels, motels, car and truck rental agencies, and storage rental facilities upon the assertion that there were "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign or an agent of a foreign power."

- Section 215 expands the authority to include not only business records but any tangible item regardless of the business or individual holding the item and upon the assertion that the records or items are sought in an effort to obtain foreign intelligence (not based solely on the protected First Amendment activities) or in a terrorism investigation.

Section 218

- Prior to the Act, FISA wiretap or search warrant applications were required to certify that *the primary purpose* for seeking the order was to obtain foreign intelligence information. This led to the belief that FISA required a wall of separation between law enforcement and intelligence investigations.

- Section 218 authorizes FISA wiretap or search warrant applications to certify that the acquisition of foreign intelligence information is *a significant purpose* of the order, rather than *the primary purpose*.

Section 225

- Section 225 provides immunity from civil liability to those who assist in the execution of a FISA wiretap order.

- Prior to the Act, FISA provided immunity to those who assist in the execution of a FISA pen register or trap and trace device order.
  - Federal wiretap law provides immunity to those who assist in the execution of a law enforcement interception order.

Section 6001 of P.L. 108-458

- Prior to enactment of this provision, the definition of an "agent of a foreign power" under FISA included individuals preparing for or engaging in international terrorism for or on behalf of a foreign power.

- Section 6001 of P.L. 108-458 eliminates the requirement that an "agent of a foreign power" be preparing for or engaging in international terrorism *for or on behalf of a foreign power* – as long as the person is not a U.S. person. The purpose of this section is to permit surveillance of individual terrorists without requiring a special showing that the non-U.S. person is affiliated with a foreign power.